BE INFO TECH 3rd YEAR 2nd SEMESTER EXAMINATION 2024

Information Security

Time: 3 Hours

Full Marks: 100

Answer All Questions

[Please show all intermediate steps clearly and elaborately. Do not skip any steps]

1.a) Illustrate and Explain Replay Attack and Denial of Service Attack. How can these attacks be prevented?

b) Illustrate and Explain Unforgettable Substitution Cipher. ((4+1)+5) **[CO1]**

2.a) Using Euler's Theorem, find the multiplicative inverse of 7 in Z_{36}.

b) How many primitive elements are there in the group (Z^*_{19}, X)? Identify the first primitive element of this group.

c) Using Numerical Examples, explain Euler's Criterion. (3+(2+2)+3) **[CO2]**

3.a) Illustrate the concept of Avalanche Effect in DES.

b) Using a proper diagram, explain the structure of each round in AES during the encryption phase.

c) Using a proper diagram, explain the permutation phase in AES during the encryption. (4+3+3) **[CO3]**

4.a) With regard to the RC4 Stream Cipher, Illustrate how the S and T vector is initialized.

b) List down the modes of operation of a Modern Block Cipher.

c) Illustrate your understanding about Ciphertext Stealing. (3+2+5) **[CO3]**

5.a) Using relevent numerical examples, explain Diffie-Hellman Key Exchange Algorithm.

b) Using relevent numerical examples, explain ElGamal Cryptosystem.

c) With regard to the RSA algorithm, Illustrate your understanding about Plaintext Attacks.
(3+3+4) **[CO4]**

6.a) For the Short-Weierstrass Elliptic Curve $E_{23}(3,9)$, Identify the first 5 points (with respect to x).

b) For the elliptic curve E_{23} (1, 1), the three different points are; P(5, 4), Q(18, 20) and R(18, 3). The (P + Q) is (9, 7). What will be the value of (P – R)? Justify your answer.

c) Illustrate and Explain the concept of ECDLP. (4+3+3) **[CO4]**

7.a) Write down the six properties of a Hash Function.

b) Discuss the differences between MDC and MAC. Explain the scenarios with examples, where they will be helpful.

c) Discuss the differences between HMAC and CMAC. Explain the scenarios where they can be used. (3+4+3) **[CO5]**

8.a) In a certain Security Scheme, the Sender encrypts the message with a Key (known to the receiver also). The sender then computes the Hash of the encrypted output. This Hash value is further encrypted by another Key (known to the receiver also). The sender then sends this output and the output of the first encryption to the receiver.

With regard to this Security Scheme, what objectives are being achieved here? Justify your answer.

b) List down the various methods of Password based Entity Authentication.

c) Illustrate and Explain all the methods of Password based Entity Authentication as mentioned above in (b).
(3+1+6) **[CO5]**

9.a) Illustrate and Explain a Simple Protocol by which Alice and Bob can exchange messages using a symmetric key cryptosystem taking the help of a KDC.

b) Illustrate and Explain Needham-Schroeder Protocol.

c) Illustrate and Explain Otway-Rees Protocol.

(2+4+4) **[CO5]**

10.a) Image scrambling is a very basic method for Image Encryption. List down the various SCAN patterns used in Image Scrambling. Illustrate one of the methods in detail.

b) Pixel Sieve Method is another technique used in Image scrambling. Illustrate this method in detail.

c) What is Information Entropy Analysis?

((1+4)+3+2) **[CO6]**